CLAIMS

What is claimed is:

1. A method of encryption, comprising:

(a) partitioning an input message into matrix elements;

(b) computing the determinant of said matrix;

(c) encrypting said determinant; and

(d) multiplying said matrix by said encrypted determinant.

2. The method of claim 1, further comprising:

(a) prior to step (a) of claim 1, preprocessing said input message wherein said preprocessing includes a permutation of the message.

3. The method of claim 1, wherein:

(a) said permutation of step (a) of claim 2 is generated by a hash of said input message.

4. The method of claim 1, wherein:

(a) said permutation of step (a) of claim 2 is generated by a random sequence.

5. The method of claim 2, wherein:

(a) said preprocessing of step (a) of claim 2 includes exclusive ORing said message after permutation with generators of said permutation.

6. The method of claim 1, wherein:

(a) said encrypting of step (c) of claim 1 is public-key encryption.

7. The method of claim 6, wherein:

(a) said public-key encryption is RSA.

8. The method of claim 1, wherein:

(a) said partitioning of step (a) of claim 1 first fills the principal diagonal of said matrix.

9. A method of encryption, comprising:

(a) preprocessing an input message wherein said preprocessing includes a permutation of the message; and

(b) encrypting said preprocessed message with a block-based encryption method which has blocks smaller than said message.

10. The method of claim 9, wherein:

(a) said permutation of step (a) of claim 9 is generated by a hash of said input message.

11. The method of claim 9, wherein:

(a) said permutation of step (a) of claim 9 is generated by a random sequence.

12. The method of claim 9, wherein:

(a) said encryption of step (b) of claim 9 is a public key encryption.

13. A method of decrypting, comprising:

(a) computing the determinant of a matrix-based encrypted message matrix;

(b) decrypting said determinant; and

(c) multiplying said matrix by the results of step (b).

14. The method of claim 13, wherein:

(a) when said matrix-based encrypted message of step (a) of claim 13 had preprocessing including a permutation, applying the inverse of said permutation to the results of step (c) of claim 13.